UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The iPhone XS Max, S/N: C39XP397MKPHK and the iPad, S/N: WI3XDJKGTV, currently located at 1201 NE Lloyd Boulevard in Portland, Oregon

Case No. 3:24-mc-00556 A-B

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

The iPhone XS Max, S/N: C39XP397MKPHK and the iPad, S/N: WI3XDJKGTV, currently located at 1201 NE Lloyd Boulevard in Portland, Oregon, as described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2261A(2)(B)	Stalking

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Rebecka Brown, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 4:18 pm a.m./p.m. *(specify reliable electronic means)*.

Date: 05/23/2024

Judge's signature

City and state: Portland, Oregon

Hon. Jeffrey Armistead, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched are the following devices, which are currently located on the premises of the Northwest Regional Computer Forensics Laboratory, 1201 NE Lloyd Boulevard in Portland, Oregon:

a. **iPhone XS Max, S/N: C39XP397MKPHK**

b. **iPad, S/N: WI3XDJKGTV**

ATTACHMENT B

Items to Be Seized

1. All records on the Devices described in Attachment A that relate to violations of Title 18, United States Code, Section 2261A(2)(B), which prohibits the use of any interactive computer service or electronic communication service or electronic communication system of interstate commerce to harass, intimidate, or place under surveillance another person, including:

a. Evidence of any social media programs or applications used to post or send communications, including date and time of installation, usage, and messages;

b. Evidence of internet usage specifically as it relates to Title 18, United States Code, Section 2261A(2)(B), including dates and times of usage; IP addresses; and usernames and passwords used to access the internet or any accounts via the internet;

c. All video recordings and images depicting suspected victims of Title 18, United States Code, Section 2261A(2)(B);

d. All records and information, including written or electronic correspondence or communications, pertaining to harassing and intimidating communications, or any attempt to commit any such offense;

e. All records or information naming or identifying victims of Title 18, United States Code, Section 2261A(2)(B);

/ / /

/ / /

f. Any records of Internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the Internet;

g. All records or information referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing harassing or threatening communications, including chat logs, call logs, address books or contact list entries, and digital images sent or received;

h. All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not in and of themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 USC 2256, such as images of minors depicted in underwear or partially undressed; and

i. Storage media used as a means to commit or facilitate the violations described above.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history. Records evidencing the use of the Internet, including:

a. Records of Internet Protocol addresses used.

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms

that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

Search Procedure

4. The examination of the Devices may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

5. The initial examination of the Devices will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Devices or images do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may

continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and it is determined that the Devices do not contain any data falling within the ambit of the warrant, the government will return the Devices to the owner within a reasonable period of time following the search and will seal any image of the Devices, absent further authorization from the Court.

8. The government may retain the Devices as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Devices and/or the data contained therein.

9. The government will retain forensic images of the Devices for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

STATE OF OREGON)
) ss: AFFIDAVIT OF REBECKA E. BROWN
County of Multnomah)

Affidavit in Support of an Application Under Rule 41
for a Warrant to Search and Seize Evidence Including Digital Evidence

I, Rebecka E. Brown, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed for approximately fifteen years. I am currently assigned to the FBI's Portland Field Office. As a federal law enforcement officer, I am authorized to investigate and make arrests for violations of federal law, and to apply for federal search warrants. I graduated from the FBI Academy at Quantico, Virginia, after completing a 19-week course of instruction. I have acquired knowledge and information about criminal conduct and investigation from many sources, including formal and informal training, other law enforcement officers, investigators, informants, persons who I have interviewed, and my participation in numerous investigations. I received specialized training in investigating a range of offenses from violent crime to financial crime. I have investigated matters involving the sexual exploitation of children, including the online sexual exploitation of children, particularly as it relates to violations of Title 18, United States Code, Sections 2252A and 2422, as well as other sexually motivated cybercrimes and stalking. I am part of the Portland Child Exploitation Task Force (CETF), which includes FBI Special Agents and Task Force Officers from Portland and Hillsboro, Oregon. The CETF is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation facilitated by an online computer. As part of my duties as a federal agent, I work with local, state, and other federal agencies on joint investigations of federal offenses, to include financial crimes.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of the following devices, which are presently in secure law enforcement custody at the Federal Bureau of Investigation, 9109 NW Cascades Parkway, Portland, Oregon 97220:

a. **iPhone XS Max, S/N: C39XP397MKPHK** (hereinafter, "**iPhone**")

b. **iPad, S/N: WI3XDJKGTV** (hereinafter, "**iPad**")

3. As set forth below, I have probable cause to believe that the items set forth in Attachment B constitute evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2261A(2)(B), which prohibits the use of any interactive computer service or electronic communication service or electronic communication system of interstate commerce to harass, intimidate, or place under surveillance another person.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

5. It is a violation of 18 U.S.C. § 2261A(2)(B) for any person, with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to injure, harass, or intimidate another person, to use the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of

interstate or foreign commerce to engage in a course of conduct that places that person in reasonable fear of the death of or serious bodily injury to a person or certain specified animals, or that causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to that person, an immediate family member of that person, or a spouse or intimate partner of that person.

Statement of Probable Cause

6. On May 17, 2023, agents seized the Subject Devices during the execution of a federal arrest warrant for MERKLE in Kings Mountain, North Carolina. Agents in the FBI's Charlotte Field Office shipped the Subject Devices to the Portland Field Office to be forensically analyzed. On August 24, 2023, the Honorable Stacie F. Beckerman signed a federal search warrant authorizing the search of the Subject Devices. Device 3, a Dell Latitude 9420 computer owned by MERKLE's former employer, was examined by the Northwest Regional Computer Forensic Laboratory (NWRCFL), but no data responsive to the warrant were located. On August 31, 2023, I examined Device 4, and found no data responsive to the warrant. I took Devices 1 and 2 to the NWRCFL for examination on September 5, 2023. Initially, a valid passcode for the Devices was not located, so the NWRCFL attempted to brute force Device 1, an iPhone XS Max. After Device 1 was unlocked, the plan was to use that passcode to attempt to unlock Device 2. In early 2024, while reviewing case notes, I located a potential passcode for Device 1. I contacted the NWRCFL forensic examiner assigned to the case who used the passcode to unlock the device. The passcode also worked on Device 2. Devices 1 and 2 were not examined due to the warrant expiring. As such, I seek the Court's permission to conduct the search of the **Subject Devices** that was authorized under the original warrant but was never carried out.

7. On September 6, 2018, an adult victim ("AV1") reported via the FBI's Public Access Line that an unknown individual, later identified as DOUGLAS ARTHUR MERKLE, was threatening her and possessed nude images of her that AV1 originally posted anonymously to a subreddit called "Gone Wild." In a subsequent interview, AV1 relayed that she posted the nude and semi-nude images to the aforementioned subreddit when she was between the ages of seventeen and nineteen years old. The images were not sexually explicit but depicted AV1 in her underwear and in various stages of nudity. AV1 posted the images for personal amusement and did not divulge her true name, posting the images instead under a Reddit username. In approximately October 2014, AV1 stopped posting images on the subreddit and focused on school.

8. In approximately March 2018, nearly four years after her last post to the subreddit group, AV1 began getting threatening Reddit messages and email messages from an unknown person (hereinafter "the Subject") using generic usernames and email addresses. The Subject requested that that AV1 post additional nude images or he would distribute her previously posted anonymous images to her friends and colleagues. AV1 declined to post or send the Subject more images, which angered him. AV1 recalled the subject making a veiled threat, such as, "I'll see you on the front page" or something similar. AV1 didn't know what it meant but took as a threat.

9. On March 12, 2018, the Subject sent the following message to AV1:

---------- Forwarded message ---------
From: Blank Name <myblankname@outlook.com>
Date: Mon, Mr 12, 2018 at 8:58 AM
Subject: Re:
To: [redacted]
Why so angry??

[end]

10. That same day, using the email account gingerguynot93@gmail.com, the Subject threatened to send a message to the Mathematics Department at AV1's college that contained a link to AV1's images. Specifically, he emailed AV1 a link to the mathematics faculty at the school she attended and asked "Have any of these people been on reddit? I wonder if I send them your links if they can help you remove them."

11. AV1 reported the harassment to campus police and to Portland Police Bureau. Both agencies advised her to tell the Subject to cease the behavior and never contact her again, which she did:

> ---------- Forwarded message ---------
> From: [redacted]
> Date: Tue, Mar 13, 2018 at 7:35 PM
> Subject: Re:
> To: blank name <gingerguynot93@gmail.com>
>
> What you are doing is considered a felony in the state of Oregon. If you continue to contact me or attempt to contact me in any way, shape or form, legal action will be taken against you.
>
> Do not contact me again on any platform.

12. Between March 14th and May 30th, 2018, AV1 received the following messages from the Subject:

> ---------- Forwarded message ---------
> From: blank name gingerguynot93@gmail.com
> Date: Wed, May 30, 2018 at 1:17 PM
> Subject: Re:
> To: [redacted]
>
> Still mad?
>
> On Thursday, March 29, 2018, blank name <gingerguynot93@gmail.com> wrote:

> Allllllll your imgur stuff is STILL up and you can STILL get to from Reddit.
>
> But I'm an asshole.
>
> On Wednesday, March 14, 2018, blank name <gingerguynot93@gmail.com>
>
> wrote:
>
> You need to delete this, dummy:
>
> [link to AV1's images posted on the subreddit]
>
> [end]

13. On August 31, 2018, the Subject, posing as AV1, sent a suggestive message to AV1's college mentor at the mentor's official university email address (redacted). The Subject attached a "selfie" image of AV1 wearing only a bra and underwear.

> ---------- Forwarded message ---------
> From: Change Name <Myblankname@outlook.com>
> Date: Fri, Aug 31, 2018 at 9:40 AM
> Subject:
> To: [redacted]lipor@pdx.edu
>
> can we? I've only got a couple weeks
>
> [end]

14. Believing that AV1 sent the message, AV1's mentor reached out to her to ask if she was "okay" and advised her that the email was highly inappropriate. AV1 recalled being 'horrified" and shaken by the situation, explaining to her mentor that she didn't send the message. AV1 described embarrassment and feelings of being violated by the Subject's actions. AV1 saw this as an attempt to discredit her and ruin her reputation.

15. A few weeks after sending the picture and suggestive message to AV1's college mentor, the Subject sent the following message to AV1:

> ---------- Forwarded message ---------
> From: Change Name Myblankname@outlook.com

Date: Wed, Sep 26, 2018 at 11:43 AM
Subject:
To: [redacted] kathleen.joslyn@pcc.edu

I want to be in you. i want to cum in you. I want to be under you and over you and behind you and on top of you and next to you.
I can't stop thinking about fucking you. I can't stop thinking about you.

16. The Subject continued to harass AV1 into 2019, sending the following messages:

From: Change Name Myblankname@outlook.com
Date: Tue, 29 Jan 2019 16:36:54 +0000
To: [redacted] kathleen.joslyn@pcc.edu
Subject:

i want to cum inside of you.

From: The George Liveatfivethedive@outlook.com
Date: Thu, 5 Dec 2019 18:16:04 +0000
To: [redacted] kathleen.joslyn@pcc.edu
Subject:

[AV1's name]!!

From: Change Name Myblankname@outlook.com
Date: Thu, 5 Dec 2019 17:31:29 +0000
To: [redacted] kathleen.joslyn@pcc.edu
Subject:

psssssst

[end]

17. AV1 reported feeling immense stress over the ongoing harassment and lived in fear of the Subject's actions. In April 2020, AV1 accepted an internship position with a prominent United States Government contractor in a specialized industry. Almost a year later, on April 29, 2021, AV1 received the following message from the Subject (AV1's name and employer redacted):

---------- Forwarded message ---------
From: Last First lastfirstnameagain@gmail.com
Date: Tue, Apr 27, 2021 at 11:09 AM
Subject:
To: Kathleen.joslyn@pdx.edu

[AV1's name]-OMG! [AV1's employer] WOW!

[end]

18. AV1 was distressed to learn that the Subject had discovered where she worked. Although she was embarrassed, AV1 decided to tell her new employer about the Subject's harassment and his attempts to damage her reputation. AV1 felt her employer needed to know that the Subject may send messages to company employees in an attempt to discredit her. AV1 reported the harassment to the company's security office and to her supervisor.

19. The Subject continued to harass AV1 until at least August of 2021. On August 19, 2021, AV1 received a message from lastfirstnameagain@gmail.com that contained only her name with the last letter repeated numerous times, as though the sender were calling her name (e.g., "Emilyyyyyyyyyyyyyyyyyyy").

20. On June 21, 2021, Google responded to a federal grand jury subpoena requesting subscriber information for the following Google accounts: gingerguynot93@gmail.com and lastfirstnameagain@gmail.com. Account information for gingerguynot93@gmail.com, revealed an alternate email and recovery email account of saku93@yahoo.com. The last login to gingerguynot93@gmail.com was reportedly '2019-07-06 15:11:15 UTC.' Numerous logins were reported for lastfirstnameagain@gmail.com, which listed an account creation date of 04/27/2021 at 17:00:37 UTC (10:00 A.M. Pacific Standard Time "PST"). This account creation date corresponds with AV1's receipt of two emails from the account.

21. A login to lastfirstnameagain@gmail.com was reported on May 19, 2021, at 19:30:09 UTC (12:30 P.M. PST). Seven minutes later, AV1 received the following email:

> ---------- Forwarded message ---------
> From: Last First lastfirstnameagain@gmail.com
> Date: Wed, May 19, 2021 at 12:37 PM
> Subject:
> To: Kathleen.joslyn@pdx.edu
>
> [AV1], [AV1], tasty [AV1]….
>
> [end]

22. According to neustar (Neustar, Inc), IP address "173.226.84.254," which was associated with the aforementioned logins, resolved to Kings Mountain, North Carolina. The carrier was identified as TW Telecom Holdings Inc - Level 3 parent LLC, which, according to online queries, is owned by CenturyLink.

23. Online queries for saku93@yahoo.com, the account linked to gingerguynot93@gmail.com, revealed several online accounts associated with "saku93," including an ImageFap account. The ImageFap profile for "saku93" contained three (3) "Galleries" that were uploaded by the user. One gallery was titled, "Uncategorized," and contained a folder named, "[AV1's first name] [AV1's Reddit username]." This folder contained numerous images of AV1, some of which were fully or partially nude and some that were apparently collected from publicly available social media accounts.

24. A query in Accurint revealed that Douglas Arthur MERKLE II ("MERKLE"), date of birth XX/XX/1975, uses the email address saku93@yahoo.com. MERKLE resides at 4819 Summerside Drive, Clover, South Carolina. Accurint reported a telephone number of 704-200-0151. This is the same phone number MERKLE listed on his résumé, which was posted online via LinkedIn.

25. As of March 31, 2023, MERKLE's LinkedIn profile lists him as an "Information Technology Site Lead" at Albemarle Corporation in Kings Mountain, North Carolina. MERKLE's profile indicates that he's been "Full-time" in that capacity since January 2022. Under the "Experience" section, MERKLE also listed himself as an "IT Consultant" in the Charlotte, North Carolina area. Albermarle's website indicates they have offices in Charlotte and Kings Mountain, North Carolina.

26. MERKLE's date of birth matches the date of birth associated with the ImageFap profile for "saku93." Also notable is that MERKLE claims to work for Albemarle, which has an office in Kings Mountain, North Carolina, the same geolocation for the IP address accessing the account, lastfirstnameagain@gmail.com. MERKLE's residence in Clover/Lake Wylie, South Carolina, is approximately fifteen (15) miles from Kings Mountain, North Carolina.

27. On March 7, 2023, a federal grand jury in the District of Oregon indicted MERKLE on one (1) count of Stalking in violation of 18 U.S.C. § 2261A(2)(B). *See United States v. Douglas Arthur Merkle*, II, 3:23-cr-66-HZ (D. Or.) (unsealed June 15, 2023). The following day, an arrest warrant was issued for MERKLE.

28. NCIC queries conducted in March 2023, for MERKLE revealed a January 2022 arrest in York County, South Carolina, for "Contributing to the delinquency of a minor." In a police interview, MERKLE first denied having messaged any juveniles on Snapchat, but after additional questioning, admitted to communicating with a neighborhood girl and leaving "gifts," to include alcohol, outside her residence. MERKLE was arrested on January 14, 2022. On December 13, 2022, a "Permanent Restraining Order" was issued in York County, South Carolina, ordering that MERKLE "be restrained from committing further acts of abuse or threats of abuse" against the female.

29. On May 17, 2023, MERKLE was arrested on the federal indictment by the FBI in Cleveland County, North Carolina, while on his way to work at Albemarle Corporation in Kings Mountain, North Carolina. During MERKLE's arrest, the following items were seized from his vehicle:

a. **iPhone XS Max, S/N: C39XP397MKPHK** (one of the **Subject Devices**)

b. **iPad, S/N: WI3XDJKGTV** (one of the **Subject Devices**)

c. **Dell Latitude 9420; service tag: GVGPPN3**

d. **USB storage device, Black with silver enclosure**

MERKLE was ordered released pending trial and remains out of custody. He has not requested the return of any of the devices seized during his arrest.

30. Based on my training, experience, and this investigation, I know that individuals such as MERKLE who are involved in cyberstalking often use portable electronic devices, such as mobile phones, tablets, laptops, thumb drives, and other electronic devices which are easily concealed. Here, because MERKLE has used Reddit and email accounts to communicate with AV1 with the intent to harass and intimidate her and in a manner which caused her substantial emotional distress, I know that criminal conduct has been facilitated by a computer and/or portable electronic device such as a tablet or a smartphone.

Background On Investigations of Online Stalking Offenses

31. Based on my training and experience, I know that people who engage in cyberstalking use online platforms to facilitate their conduct, including Internet-based platforms such as Reddit and Gmail. As relevant in cases such as this one, these online services allow a user to set up an account with a remote computing service that provides messaging services, methods of payment, and a means of electronic storage through which users can contact victims

and related third parties, and potentially store communications or compromising images of the victim for use as blackmail or harassment. Even in cases where online platforms are used for the storage of communications or images, evidence of the same can commonly be found on the user's internet-connected devices, even if long periods of time have passed from confirmed dates of possession or distribution.

32. Based on my training, experience, and consultation of agents experienced in cyberstalking investigations, I know that persons who engage in cyberstalking often have multiple victims, either during the same time period or sequentially over time. They collect information and images related to their victims, including web searches of their victims' names and locations, visits to websites hosting information about their victims or victims' family, friends and colleagues, and images of their victims downloaded from public websites or received through communications with the victim. This evidence is usually stored on the stalker's internet-connected devices and storage media, both actively – such as when the stalker deliberately saves an image on their cell phone or computer – and passively – such as when Google or a similar search engine records internet searches conducted on a device. When such items are found on a user's device, they can serve as direct evidence of that user's stalking of a specific victim. Such items can also help identify additional victims, and can serve as evidence of the user's knowledge, intent, motive, and identity.

33. Based on my training, experience, and consultation of agents experienced in cyberstalking investigations, I know that individuals who engage in cyberstalking maintain information, communications, and images pertaining to their victims over a long period of time and rarely, if ever, dispose of such items. This is especially true of communications directly with the victim and of compromising images of the victim, which are highly valuable to the stalker

because they give the stalker a sense of power and control over the victim and can be used to blackmail or harass the victim. The known desire of such individuals to retain information and images pertaining to their victims, together with the sense of security afforded by using computers, provides probable cause to believe that computer images and data will be retained by the stalker indefinitely. These individuals may protect such materials by passwords, encryption, and other security measures, save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted, or send it to third party image storage sites via the Internet.

Examination of Data Storage Devices

34. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant.

35. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, is often essential to conducting a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that are concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

36. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited

text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data are within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data are often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data require a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

37. *Latent Data*: Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represent electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remain on the hard drive until it is overwritten by new data.

Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file.

38. *Contextual Data*

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online

nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, and malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search Procedure

39. In searching the devices described in Attachment A, law enforcement personnel executing the search warrant will employ the following procedure:

40. Law enforcement personnel will examine the digital devices to extract and seize any data that fall within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that fall outside the scope of the warrant that they believe should be seized (e.g. evidence of other crimes), they will seek an additional warrant.

41. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized under the warrant.

42. Law enforcement personnel will perform an initial search of the digital devices within a reasonable amount of time not to exceed 120 days from the date of the execution of the warrant. If, after the initial search, law enforcement personnel determine that an original device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of the chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether a digital device contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of the execution of the warrant. The government shall complete the search of the digital devices

within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court.

43. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on a digital device do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

44. If a digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that device, and will seal any image of the device, absent further authorization from the Court.

Data to be Seized

45. In order to search for data that are capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

46. The electronic devices described above and in Attachment A hereto, presently in secure evidence storage at the Northwest Regional Computer Forensic Laboratory (NWRCFL), for contraband or the types of evidence, fruits, or instrumentalities of the crimes of stalking, as set forth in Attachment B;

47. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to upload, download, store, receive, possess, or view data related to stalking, including the web browser's history; temporary Internet files; cookies; bookmarked or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

48. The government has made no prior efforts in other judicial fora to obtain the evidence sought in this warrant other than those described above.

Retention of Image

49. The government will retain a forensic image of the electronic storage devices subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

50. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

Conclusion

51. Based on the foregoing, I have probable cause to believe that the devices described in Attachment A contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2261A(2)(B), as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the devices described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

52. This affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Mira Chernick prior to being submitted to the Court. AUSA Chernick advised me that in her opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By Phone Per Fed. R. Crim. P. 4.1
REBECKA E. BROWN
FBI Special Agent

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 4:18 p.m. on May 23, 2024.

HONORABLE JEFFREY ARMISTEAD
United States Magistrate Judge